What is claimed is:

1. A server apparatus comprising:

a key sharing processing unit configured to perform a first protocol to share a first key with a client apparatus;

an encryption/decryption unit configured to encrypt data or decrypt encrypted data by use of the first key obtained from said key sharing processing unit;

a communication unit configured to transmit to said client apparatus, data which was encrypted by said encryption/decryption unit or receive from said client apparatus, data which was encrypted by using the first key; and

said key sharing processing unit having:

a first reception unit configured to receive key information from said client apparatus, said key information including the first key or data which becomes a basis for generating the first key, and said key information being encrypted with a second key,

a transmission unit configured to transmit a request to decrypt the key information to a key management apparatus which maintains a third key necessary for decrypting the key information; and

a second reception unit configured to receive the first key or the data which becomes a basis for generating the first key from said key management apparatus.

2. The server apparatus according to claim 1, further comprising a key generation unit configured to generate the first key, from the data which becomes a basis for generating the first key.

3. The server apparatus according to claim 1, wherein a connection between said server apparatus and said key management apparatus is through a dedicated network isolated from said client apparatus.

4. The server apparatus according to claim 1, wherein data transferred to said key management apparatus is encrypted before transfer.

5. The server apparatus according to claim 4, wherein a second protocol for sharing a fourth key which is used for encrypting data transferred to said key management apparatus is as same as the first protocol.

6. The server apparatus according to claim 1, wherein said transmission unit transmits all requests to one predetermined key management apparatus.

7. The server apparatus according to claim 1, wherein said transmission unit transmits the request to one predetermined key management apparatus selected from a plurality of key management apparatuses.

8. The server apparatus according to claim 1, further comprising a storing unit configured to store authentication information used to authenticate said server apparatus with said client apparatus.

9. The server apparatus according to claim 1, further comprising an obtaining unit configured to obtain authentication information used for server authentication with said client apparatus from said key management apparatus.

10. The server apparatus according to claim 1, wherein the server apparatus stores the second key temporarily, but does not stores the third key at any time.

11. A key management apparatus comprising:

a reception unit configured to receive a request for decrypting key information from a server apparatus, said key information including a first key or data which becomes a basis for generating the first key, and said key information being encrypted with a second key;

a storing unit configured to store a third key which is necessary for decrypting the key information;

a decryption unit configured to decrypt the key information with the third key and obtain the first key or the data which becomes a basis for generating the first key, after receiving the request; and

a transmission unit configured to transmit to said server apparatus the first key or the data which becomes a basis for generating the first key,

wherein said server apparatus and a client apparatus are able to share the first key.

12. The key management apparatus according to claim 11, wherein said key information is encrypted by said client apparatus.

13. The key management apparatus according to claim 11, wherein a connection between said key management apparatus and said server apparatus is

through a dedicated network which is isolated from said client apparatus.

14. The key management apparatus according to claim 11, wherein data to be transferred to said server apparatus is encrypted before transfer.

15. The key management apparatus according to claim 14, wherein a protocol for sharing a fourth key used to encrypt data transferred to said server apparatus is the same as a protocol for sharing said first key between said server apparatus and said client apparatus.

16. The key management apparatus according to claim 11, wherein the key management apparatus is connected to a plurality of server apparatuses, and the second key and the third key are commonly used for the plurality of server apparatuses.

17. The key management apparatus according to claim 11, wherein the key management apparatus is connected to a plurality of server apparatuses, and the second key and the third key are unique to one server apparatus of the plurality of server apparatus.

18. The key management apparatus according to claim 11, further comprising:

a second storing unit configured to store authentication information which said server apparatus uses for server authentication with said client apparatus;

a second reception unit configured to receive, from said server apparatus, an authentication request for the authentication information; and

a second transmission unit configured to transmit the authentication information to said server apparatus, after receiving the authentication request.

19. An encrypted communication method comprising:

receiving key information from a client apparatus, said key information including a first key or data which becomes a basis for generating the first key, and said key information being encrypted with a second key;

transmitting a request to decrypt the key information to a key management apparatus which stores a third key necessary for decrypting the key information;

receiving the first key or the data which becomes a basis for generating the first key from said key management apparatus;

if the key information is a basis for generating the first key, generating the first key from the basis; and

encrypting data using the first key and transmitting the data encrypted with the first key to said client apparatus, or receiving data encrypted with the first key from said client apparatus and decrypting the data encrypted with the first key.

20. The encrypted communication method according to claim 19, wherein

encrypting said key information comprises using an asymmetric encryption process, and

the second key is a public key and the third key is a private key.

21. An encrypted communication method comprising:

receiving a request for decrypting key information from a server apparatus,

said key information including a first key or data which becomes a basis for generating the first key, and said key information being encrypted with a second key;

storing a third key which is necessary for decrypting the key information;

decrypting said key information with the third key and obtaining the first key or the data which becomes a basis for generating the first key, after receiving the request; and

transmitting to said server apparatus the first key or the data which becomes a basis for generating the first key,

wherein the server apparatus and a client apparatus are able to share the first key.

22. The encrypted communication method according to claim 21, wherein

decrypting said key information comprises using an asymmetric decryption process, and

the second key is a public key and the third key is a private key.

23. A communication program for communicating to a client computer, comprising:

a key sharing processing program code configured to perform a protocol for sharing a first key with a client computer;

an encryption/decryption program code configured to encrypt data or decrypt encrypted data using of first key obtained from said key sharing processing program code;

a communication program code configured to transmit to said client apparatus, data encrypted by said encryption/decryption program code or configured to receive,

from said client apparatus, data which was encrypted using the first key; and

said key sharing processing program code having:

a first reception program code configured to receive key information from said client apparatus, said key information including the first key or data which becomes a basis for generating the first key, and said key information being encrypted with a second key;

a transmission program code configured to transmit a request to decrypt the key information to a key management apparatus which stores a third key necessary for decrypting the key information; and

a second reception program code configured to receive the first key or the data which becomes a basis for generating the first key from said key management apparatus.

24. A communication program for managing key information, comprising:

a first reception program code configured to receive a request for decrypting key information from a server apparatus, said key information including a first key or data which becomes a basis for generating the first key, and said key information being encrypted with a second key;

a first storing program code configured to store a third key necessary for decrypting the key information;

a decryption program code configured to decrypt said key information with the third key and obtain the first key or the data which becomes a basis for generating the first key, after receiving the request; and

a first transmission program code configured to transmit the first key or the

data which becomes a basis for generating the first key to said server apparatus,

wherein said server apparatus and a client apparatus are capable of sharing the first key.

25. A secure communication system, comprising:

a network;

a server apparatus connected to said network and capable of exchanging data with a client apparatus, said server apparatus having a certificate which includes a public key;

a client apparatus connected to said network, and capable of exchanging data with said server apparatus and receiving said certificate from said server apparatus;

a key management apparatus connected to said network, said key management apparatus including:

a first reception unit configured to receive a request for decrypting key information from said server apparatus, said key information including a first key or data which becomes a basis for generating the first key, and said key information being encrypted with the public key by said client apparatus;

a first storing unit configured to store a private key which is necessary for decrypting the key information;

a decryption unit configured to decrypt the key information with the private key and obtain the first key or the data which becomes a basis for generating the first key, after receiving the request; and

a first transmission unit configured to transmit to said server apparatus the first key or the data which becomes a basis for generating the first key.